Intelligence Community Public Key Infrastructure (IC PKI)

MITRE

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2002		**00-00-2002 to 00-00-2002**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Intelligence Community Public Key Infrastructure (IC PKI)	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **MITRE Corporation,202 Burlington Road,Bedford,MA,01730-1420**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

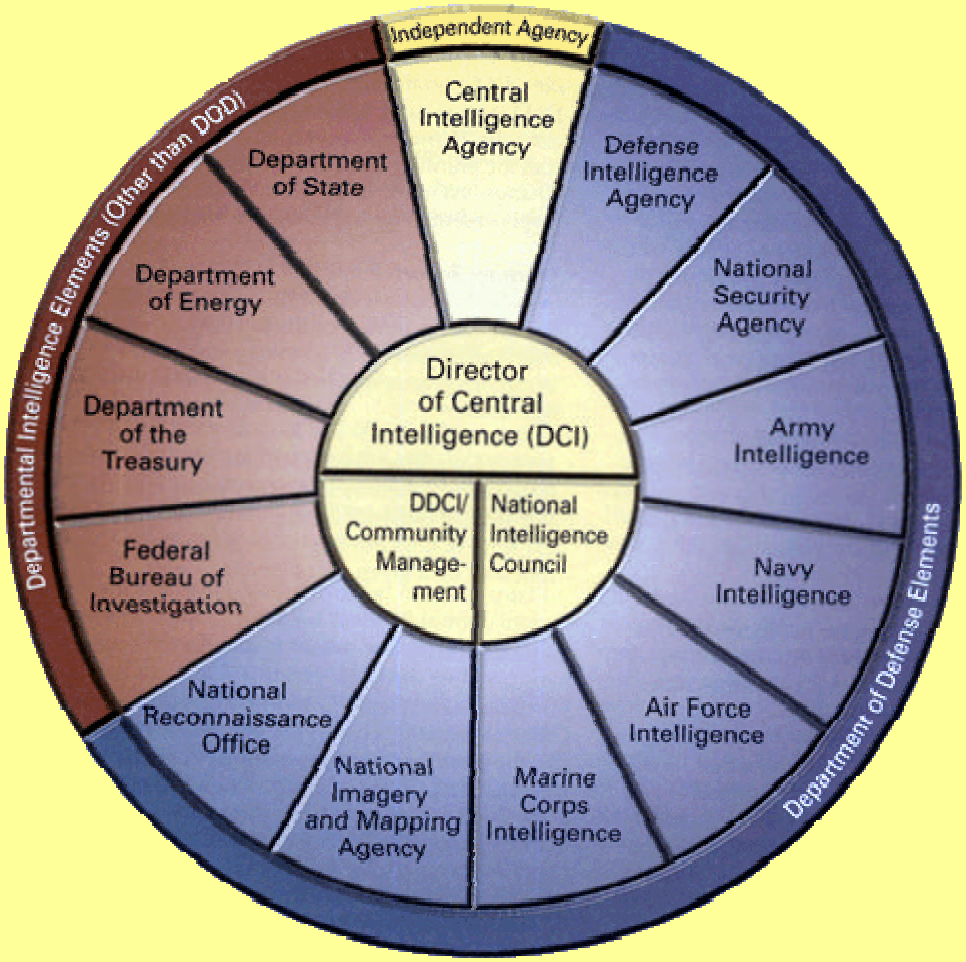
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**19**	

Outline

- The US Intelligence Community
- Why is PKI needed on CLASSIFIED networks?
- What is in an IC PKI Certificate?
- Current IC PKI Status
- Notional IC PKI Topology
- MITRE IC PKI/FSD Laboratory
- Certificate Validation
- IC PKI Requirements and Issues
- Conclusion

MITRE

The US Intelligence Community



Ref: CIA website http://www.cia.gov/ic/contents.html

MITRE

Why is PKI Needed on CLASSIFIED Networks?

- The ability to establish more secure areas on CLASSIFIED networks is essential to wider release and dissemination of data to the end users
  - Data dissemination that needs to be tracked and controlled
  - Data restricted to those with a “need to know”
  - Compartmented data (beyond the level of the network)
  - Originator-controlled data
  - Data restricted to those on a “by name” access control list

MITRE

Why is PKI Needed on CLASSIFIED Networks? (cont)

- PKI-enabled applications can include:
  - Secure messaging applications
    - Who sent me that message?
  - Secure Web access and Communities of Interest (COIs)
    - How do I keep other people from viewing this data?
  - Release authorities and disclosure procedures
    - How do I know I can release this information?
  - Mobile Code and object signing
    - Who authored this applet and can it be trusted?
  - Virtual Private Networks (VPN)
    - How can I have a (more) secure connection?
  - Collaborative toolkits
    - Can we establish a (more) secure VTC?

MITRE

Why is PKI Needed on CLASSIFIED Networks? (cont)

- In addition, agencies are allowed to use the IC PKI certificate for internal purposes
  - Approval documents
  - Electronic workflow applications
  - Restricted access directories and documents
  - Financial forms

MITRE

IC Communities of Interest

Network Access Control Level	Description	Access Control Mechanism	Server Management	Certificate	Technical Requirements
1	General Access	None Information available to all network users			
2	Controlled Access (Simple I & A)	Access may be controlled by non-certificate based controls			
3	Authenticated (Certificate based I&A)	Valid Community certificate required		Community	SSL
4	Restricted Membership - Distributed Control	COI access decision is managed according to rules approved by data owners and the decision process may be centralized or decentralized	Per data owner's consent	Community	SSL
5	Restricted Membership - Data Owner Controlled	COI access decision is managed by the data owner	Data Owner	Community	SSL
6	Restricted Membership - Self-Protecting Data	COI access decision is managed by the data owner	Data Owner	Data Owner designates Certificate Authority (Community or other)	Self-Protecting Data -- Data are encrypted in transit and at-rest and are only accessible by authorized user

IC PKI

MITRE

What is in an IC PKI Certificate?

Signature Certificate (required elements)

Basic Certificate			
Version		V3(2)	Identified which version of X.509 standard is being used
Serial Number		Unique integer	Identifies certificate
Issuer Signature Algorithm		sha1WithRSAEncryption	Specified signature algorithm for CA key
Issuer Distinguished Name			
Country Code	C	US	Country of certificate issuance
Organization	O	U.S. Government	Per federal PKI guidelines
Organizational Unit 1	OU1	DCI	Cabinet-level organization
Organizational Unit 2	OU2	CIA	Agency
Common Name	CN	CIA-IC-PKI	Name of agency certificate authority
Validity Period		012400ZMAY00-012400ZMAY03	User certificates are valid for up to three years
Subject Distinguished Name			
Country Code	C	US	Country of certificate issuance
Organization	O	U.S.Government	Per federal PKI guidelines
Organizational Unit 1	OU1	DCI	Cabinet-level organization
Organizational Unit 2	OU2	CIA	Agency
Common Name	CN	MacGarrigle.Ellen.F.1234UYTF	Unique name within an agency (at agency discretion)
Subject Public Key Information		1024 RSA key modulus, RSA encryption	Information needed to process user's public key
Issuer's Signature		sha1WithRSAEncryption	Actual issuer key signature

MITRE

What is in an IC PKI Certificate (cont)?

Signature Certificate (required elements)

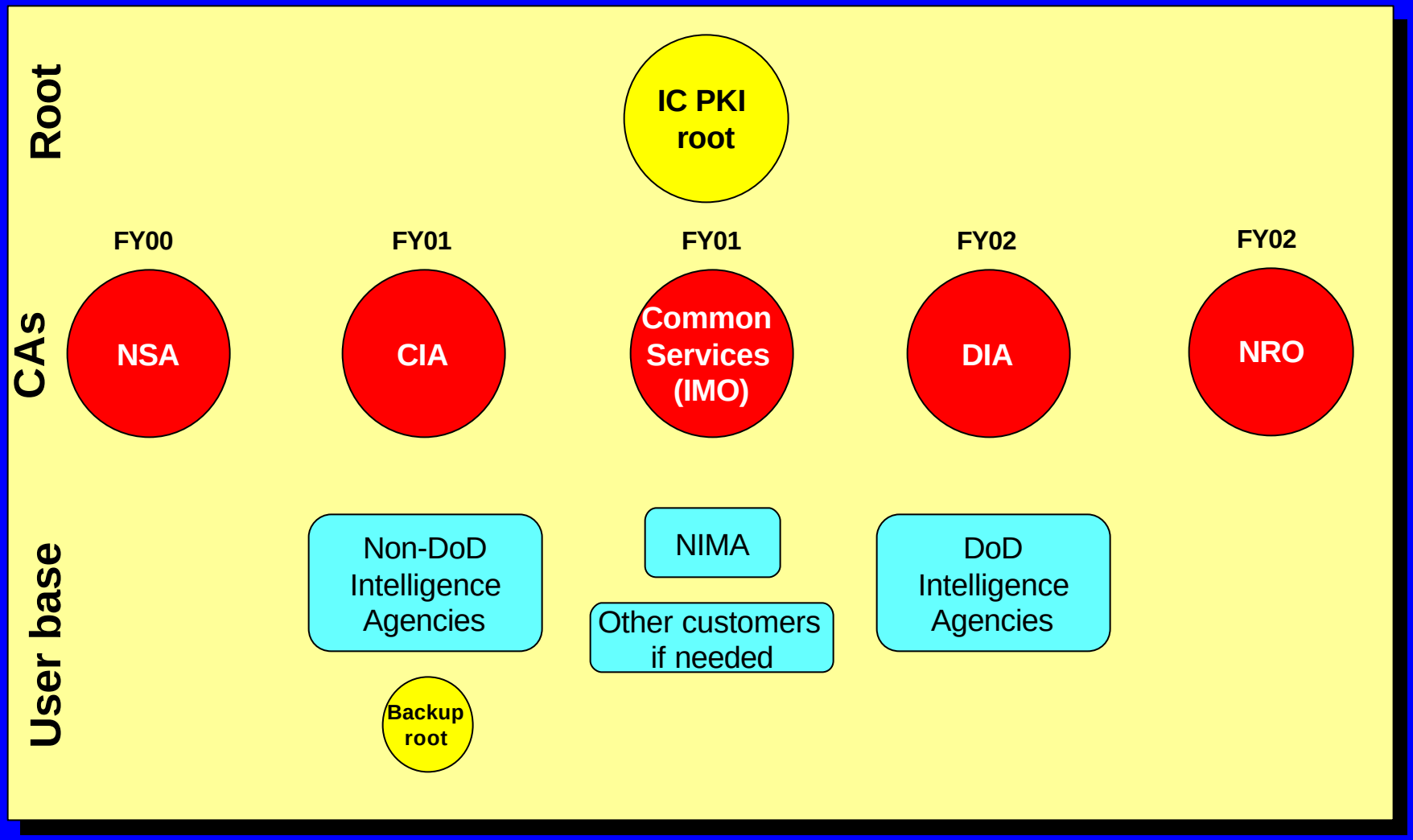
Extensions			
Key Usage		email signing certificate: digitalSignature set non-repudiation set keyEncipherment not set	Permits use for authentication and non-repudiation only when used with newer S/MIME clients
Certificate policies		*id-US-level3 ::={id-certificate-policy 7}*	*Alphanumeric code identifying governing Level 3/Level 4 PKI policy*
Subject Alternative Name		*macgari@cia*	*User's ICEmail address*
Subject Directory Attributes		*Nationality=US*	*Citizenship of user*
		EmployeeType=Contractor	*Employment status of user*

"Many legacy S/MIME clients do not enforce functional separation so both the digitalSignature and keyEncipherment flags may be set in some certificates. Since newer S/MIME clients that enforce functional separation are beginning to become available, the IC PKI shall require one S/MIME certificate with the digital signature and non-repudiation bits set and a second certificate with the key encipherment bit set for those clients." (IC PKI Certificate Policy)

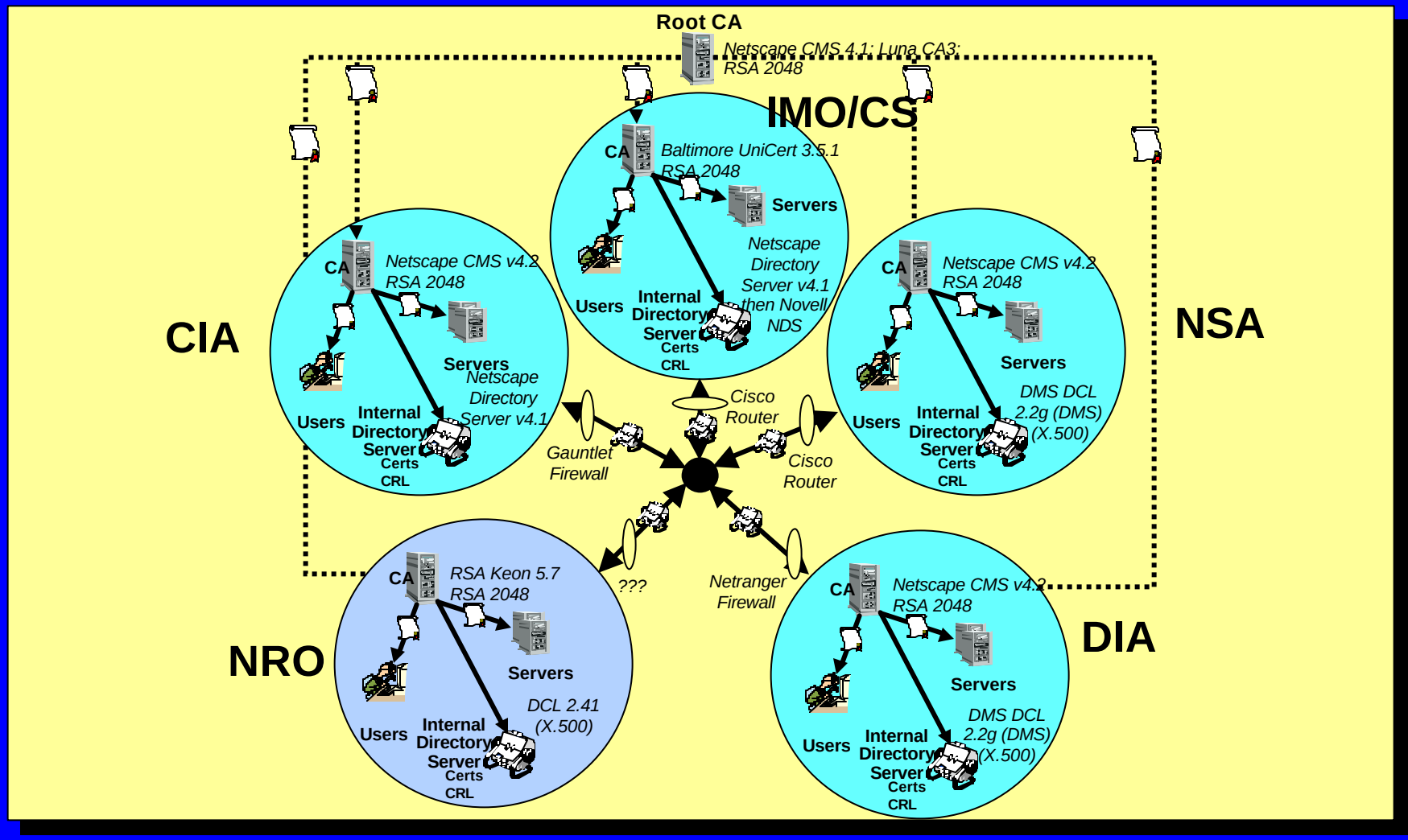
Note: fields in red italics mean required but "non-critical" fields

MITRE

Notional IC CA PKI Topology



PKI/FSD Lab Configuration



MITRE

Current IC PKI Status

- Overarching Policy signed October 1999
- Certificate Policy signed February 2000
- IC standup effort currently underway
  - Root: Interim Authority to Operate (IATO) on 24Jul00, final ATO issued 08Aug00
  - NSA: Interim Approval to Test (IATT) Aug00, IATO Sep00
  - CIA: IATT Apr01, ATO Jun01
  - Common Services (IMO) (incl NIMA): IATT Jun01, IATO Sep01, ATO Dec01
  - DIA: IATT August 2001, IATO Oct0ber 2001, planned ATO Feb02
  - NRO: Planned IATT Mar02(?), planned ATO May02(?)

Certificate Validation (cont)

- To ensure certificate validity, certificates must be verified
  - Applications may check expiration dates but other checks are not automatic
  - Certificates may be revoked for the following reasons:
    - identifying information or attributes in the end entity's certificate changes before the certificate expires;
    - the certificate subject can be shown to have violated the CP or the CPS of the CA who issued the certificate;
    - fraudulent use or suspected compromise; or
    - the user or other authorized party (as defined in the CA's CPS) asks for his/her certificate to be revoked
  - Two approaches are supported today:
    - Certificate Revocation Lists (CRLs)
    - Online Certificate Status Processing (OCSP)

MITRE

Certificate Validation (cont)

- Certificate Revocation Lists (CRLs)
  - A list of revoked certificates issued by an IC PKI CA
  - Each CA issues their own CRL
  - CRLs are periodically issued to reflect revoked certificates
    - CRLs work on a "push/pull" basis (an issuing CA periodically "pushes" the information out; other CAs periodically "pull" this information in)
    - IC PKI CP mandates a new CRL every 28 days

      Nonroutine revocations are issued within six hours
  - CRL retrieval is based on organizational need/processes
    - Community applications that understand CRLs must retrieve a CRL at least every 72 hours
  - CRLs need a central distribution point or points

MITRE

Certificate Validation (cont)

- Online Certificate Status Processing (OCSP)
  - OCSP means that a CA automatically attempts to validate a certificate each time the certificate is used
  - Each CA must maintain an OCSP lookup point wherein the relevant information is located
  - OCSP works in real time but must as a minimum meet the same mandated deadlines as CRLs (28 days/6 hours)
  - OCSP options
    - A CA may “push” the CRL to the OCSP responder
    - A CA may “push” the CRL to the FSD and the responder “pulls” it from there
    - Some CAs have built-in responders that automatically “pull” the needed data from the issuing CA
  - Few applications currently use OCSP

MITRE

IC PKI Requirements and Issues

- Lack of common IC directory
  - Extensive installed base precludes single common directory
  - Federated approaches make directory-based functionality more complex and may impose more processing overhead
  - Directory is not yet operational even though IC PKI has reached IOC
- Desire to avoid separate operations and maintenance infrastructure
  - Most O&M costs for PKI are labor-related (registration and revocation are manpower-intensive)
  - IC PKI structure mirrors DoD structures as much as possible to allow reuse of already-planned support organizations and procedures

MITRE

IC PKI Requirements and Issues (cont)

- Absolute need for key escrow
  - Required for counterintelligence purposes
- Auditing and Malicious Code Detection Policies
  - Should an encrypted message be logged and scanned at the gateway?
- Foreign (allied) national access
  - US users of foreign allied networks have a need to access US resources
- PKI deployment and training issues
  - We need good user training materials

MITRE

IC PKI Requirements and Issues (cont)

- We have a real requirement for “group” certificates with individual audit capability
  - Ease of operations makes it imperative that some messages be sent and received from common addresses and accounts
    - A virus warning would be “signed and sent” from an agency CIRT desk to prove its authenticity; a user would not have to identify John Doe as being the watch officer
    - A watch officer comes on duty to relieve another watch officer and wants to be able to read all emails sent and received from the position during that duty day
    - A question arises about a warning sent by a duty officer position six months ago; who was the individual who sent that official message?

MITRE

Conclusion

- IC PKI is on schedule to complete infrastructure deployment this year
- In 2002 IC PKI is moving toward
  - PKI enablement of applications
  - Updating original hardware and software configurations
  - User training and education
  - Interim directory deployment
  - Vendor interoperability issues

MITRE